Date: *July 27, 2018*
Source: *Medizin + Elektronik*
https://www.medizin-und-elektronik.de/medizin-40-iot/artikel/154470/

Press Report

General Data Protection Regulation:
Handling patient data is becoming more complex

Marc Schieder, CIO DRACOON GmbH

Regensburg, 27.07.2018 – Digitalization is progressing unstoppably, without omitting the health sector. Patient records have long been stored digitally and can be retrieved as required. This brings great benefits, but at the same time carries some risks.

Diagnosis: hacker attack. In spring 2016, blackmailers paralyzed the computer system of the Lukas Hospital in Neuss – without ever having setting foot in it. Instead, they infiltrated the system with a digital Trojan. At first, the ambulance staff noticed that something was wrong, and the computers in radiology were also running remarkably slowly. In other medical departments, the employees were also unable to work as usual. Some time later, a message appeared on several monitors: This data is encrypted. You should contact a special email address to get access to it again. The hospital reacted immediately, shut down all systems and switched to "manual operation".

In the end, more than 800 terminal devices were affected in the Lukas Hospital, as were servers and data storage devices. After a few days, the Ransomware could be identified and a special antivirus software could be created. Gradually, the individual systems and their subsystems were started up again – a process that lasted for weeks. And even if the people of Neuss had not responded to the blackmail attempts associated with the cyberattack, it was expensive in the end, with a total loss of almost 900,000 euros. The case shows: Digitalization also has its pitfalls, especially when it comes to protecting patient data.

Hospitals don't work without personal data

Medical data is one of the most sensitive and private pieces of information. At the same time, it is necessary that these can be exchanged quickly. Until today, most data such as patient records, laboratory results and MRI images are stored either on local servers or in cloud memories of well-known providers. The latter is particularly problematic because data stored in US data centers, for example, is not subject to the protection of local data protection laws.

Nevertheless, it is essential in the medical field to collect and work with personal patient data. This also includes the transmission of data that are processed in laboratories for further analysis. This step is often associated with considerable logistical and financial expenditure, as electronic data transmission is out of the question due to the large amount of data, so cost-intensive courier services have to be ordered instead. An intelligent cloud storage solution can counteract these problems. Assuming high data protection compliance, data can be stored securely and shared quickly and easily if required.

The current form of data use is problematic in many hospitals

While some healthcare companies still process data in physical form, most are already relying on digitized data. Digital health and patient data make everyday work easier for everyone in the healthcare sector: For staff, digitized data means that files, MRI documents or even X-ray images are quickly available. Patients benefit from shorter waiting times and individualized therapy. Currently, if such data is available digitally, it is often stored centrally on an on-premises solution. If the data is required on another device, removable storage devices are used or, if they are to be made available to several people at the same time, cloud storage providers. In case of doubt, this can also be an employee's private cloud.

This practice poses a problem both in data protection law and with regard to the workflow: First, it is cumbersome to store and share data on removable media every time you need it, and there is also the risk of losing it. If private cloud storage is used for this purpose, for example to view a file again at a later point, data protection problems also arise for the users. Recently it became known that data stored on servers of known cloud providers was not safe from access by unauthorized third parties. Particularly popular US cloud storage providers have data protection deficits: As soon as data is stored in a US-American data center, it is possible for authorities to read and store it. As long as no simple alternative is specified here, employees will continue to use these storage solutions. Away from known structures, this creates a shadow IT that is not under the control of IT administrators.

Violations of data protection are becoming expensive

Data protection, which includes not only security but also the traceability of data collection, represents a central challenge. Applied solutions are often inconsistent and often lead to problems in communication between hospitals and laboratories. The European General Data Protection Regulation (GDPR), which came into force on 25 May 2018, can make such errors in the handling of personal data very expensive due to hefty fines. Personal data is defined as any information of an identified or identifiable person, including x-rays and medication data, and as such must comply with certain data protection standards. For the use of this data, for example, the express consent of the patient must be obtained. Violations of the GDPR may result in fines of up to 20 million euros or 4% of a company's total worldwide annual turnover.

As a side effect of digitization, the number of devices accessing a network in hospitals is also increasing. This also increases the area for potential cyber attacks. This threatens not only the migration of data but also, as mentioned at the beginning, a complete blocking of access. If an attack occurs, the computer used is infected with encryption Trojans, as in the cyber attack on the Lukas Hospital in Neuss. A successful ransomware attack encrypts all data on a network. To decrypt the data again, a payment in the form of crypto currencies is common. Often, a countdown is displayed on the screen, after which either the amount of ransom to be paid increases or the data is irretrievably deleted. Such attacks are counteracted by a versioning of the cloud memory, as every deleted file is saved automatically in its last version, whereby ransom claims are no longer a danger. Even if data appears to have been completely deleted, its most recent version is still stored in the trash.

What a secure cloud storage system must be able to do
A high level of compliance with current data protection guidelines is certainly one of the most important features that cloud storage must fulfil. This also includes making personal data accessible only to authorized persons. A simple authorization system helps to provide transparency within the company as to who has been authorized for which data. Various seals certify cloud providers according to their compliance with the GDPR and their general data protection status. Particularly noteworthy are the EuroPriSe (European Privacy Seal), which distinguishes providers as GDPR-ready, the seal of approval of the ULD (Independent Centre for Data Protection Schleswig-Holstein), and ISO 27001.

In addition, the use of the cloud storage system itself should be intuitive, but at the same time secure, as it promotes acceptance in everyday life on the one hand and avoids lengthy training courses on the other. The integration of the online storage as a network drive simplifies working in already known folder structures. In addition, there are also plug-ins for Outlook that enable the secure sending of large files. But above all, specially created data rooms offer many advantages for cooperation with external project partners. Such solutions are particularly useful in research, where large amounts of data can be processed and made available in the shortest possible time.

The goal: data security and availability
In a digitalized world, the fast exchange of data is essential. The healthcare sector is also not excluded from the changes brought about by digitalization. This makes it all the more important for decision-makers to look at the opportunities that cloud storage systems bring. Since data is of the utmost importance in the health sector, the security of this data should be a priority.

Data protection in particular poses major challenges for data storage institutions and companies. Therefore, it should be ensured from the outset that the selected storage solution has a high level of compliance. Decision-makers play it safe with "Made in Germany" data storage devices: These solutions comply with both Germany's existing strict data protection laws as well as the GDPR.

The workplace in the health sector of the future will certainly be completely digitalized. All important patient data and findings will be digitally accessible and available on the mobile devices of employees. Cooperation and exchange with research and laboratories are made more efficient through improved availability of data.